효과적인 침입방지시스템 구현 참고사항들

김광훈*, 이상진*

*고려대학교, 정보보호대학원

Effective Implementation ways for Intrusion Prevention System

Gwang-hoon Kim*,Sang-Jin Lee*

*CIST, Korea Univ.

요 약

컴퓨터 기술과 네트워크 기술이 발전함에 따라 많은 네트워크들이 독립성을 가지게 되었고 이에 따라서 그 취약점들을 이용한 공격들도 늘어나고 있다. 이에 따라 침입을 탐지하는 시스템들은 많이 제안되고 제품화되고 있으나 점점 더 침입 탐지뿐만이 아니라 방지할 수 있는 침입방지시스템의 개발이 간절히 요구되고 있다. 이 논문에서는 표준이 정해져있지 않은 침입방지시스템(IPS: Intrusion Prevention System)의 설계 및 구현 시에 필요한 효과적인 방법들을 제시하고 있다.

I. 개요

급속한 정보통신 기반구조의 확산에 따라, 정보화 서비스 또한 다양한 형태로 우리의 생활과 가까워지고 있다. 이러한 정보화의 발전이 진행될수록 그 역기능 또한 증가되어 정보보안에 대한 문제가 심각하게 대두되고 있다.

얼마전 세계 유명 사이트들이 연이어 침입을 당하고 911 테러까지 발생하면서 많은 시스템 관리자들이 대응에 고심하고 있으며, 이제 해킹 문제는 정보전의 심각한 문제로까지 진행되고 있는 것이 현실이다.

컴퓨터 보안은 차단(Prevention), 탐지(Detection), 대응(Response)의 3가지 형태가 필수적이다. 그러나 지금까지의 대부분의 보안제품은 탐지기능(IDS)만 있거나 차단기능(Firewall)만 있다. 하지만 좀 더 동적으로 대응할 수 있는 시스템의 요구가 늘어나자 IPS(Intrusion Prevention System)이라는 새로운 개념이 등장하게 되고 다양한 개발방법들에 의해 제품이 생산되고 있지만 아직 개념적으로도 정리가 되어있지 않은 실정이다.

따라서 본 논문에서는 좀 더 현실적인 IPS의 개발 시에 고려해야 할 사항들을 제시할 것이다.

II. 침입방지시스템

기존의 방화벽(Firewall)이나 침입탐지시스템(IDS)의 경우, 침입 등의 공격에 그리 능동적으로 대처할 수가 없다. 방화벽의 경우 정책이 변하면 바뀔 때마다 일일이 변경을 해주어야 하고, IDS의 경우는 침입의 탐지만 하는 등, 매우 수동적일 수 밖에 없었다. 능동 보안기술이란 보안 측면에서 볼 때 침입에 대한 능동적인 대응(active response)을 의미하고, 실행 측면에서는 선처리 방어(proactive protecting) 기술을 이용한 동적 실행환경을 뜻한다. 현재 능동 보안기술은 보안시스템이 설치된 자신의 도메인에 국한하지 않고 침입에 대한 해당 트래픽의 근원지를 다양한 방법으로 입수, 근원적으로 차단해 제2, 제3의 침입을 막는데 초점을 맞추고 있다[8]. 이에 좀 더 능동적인 대처방법에 대한 필요성이 커졌는데, 그것에 응하는 것이 바로 침입방지시스템(IPS) 이다.

1. 기존 기술의 문제점.

1)침입탐지시스템(IDS)

기존의 침입탐지 시스템의 종류는 두 가지로 크게 분류될 수 있다. 하나는 네트워크 기반의 침입탐지 시스템이고 또 하나는 호스트 기반의 침입탐지 시스템이다. 이 두 가지 시스템의 문제점은 단순히 침입의 흔적을 찾기만 한다는 것이다. 동적으로 대처하는 것에는 한계가 있고, 탐지는 항상 공격기법을 데이터베이스에 저장하고 패킷을 비교해서 잡아내는 단점이 있다.

2)방화벽(Firewall)

방화벽은 네트웍 게이트웨이 서버에 위치하고 있는 일련의 연관된 프로그램들로서, 다른 네트웍의 사용자들로부터 사실 네트웍의 자원들을 보호

해준다 (이 용어는 보안정책과 함께 사용된 프로그램들에도 적용된다). 방화벽은 외부인이 자신의 공개되지 않은 자원에 접근하는 것을 막고, 자기 회사의 직원들이 접속해야 할 외부의 자원들을 통제하기 위해 기업의 인트라넷과 인터넷 사이에 설치된다.

기본적으로 방화벽은 라우터 프로그램과 밀접하게 동작함으로써, 모든 네트웍 패킷들을 그들의 수신처로 전달할 것인지를 결정하기 위해 검사하고, 여과한다. 또한 방화벽은 워크스테이션 사용자 대신 네트웍에 요청을 해주는 프럭시 서버의 기능을 포함하거나 또는 함께 상호 협력하여 동작한다.

방화벽은 네트웍의 다른 부분들과는 별개로, 특별히 지정된 컴퓨터에 설치되는 경우가 많은데, 이는 들어오는 요구가 사실 네트웍 자원으로 곧바로 전달되지 않도록 하기 위한 것이다.

방화벽의 차폐방법에는 몇 가지가 있다. 단순한 방법 중 하나는 들어오는 요구가 받아들일만한 (즉, 이전에 확인된) 도메인 이름이나 IP 주소로부터 오는 것인지를 확인하는 것이다. 이동중인 사용자들을 위해서는 보안접속절차나 인증확인 등을 통해 사설 네트웍에 원격접속 할 수 있도록 허용한다.[7]

기존의 방화벽은 차단을 하는 규칙이 존재하여, 항상 그 규칙에 의해 동작한다. 단점은 규칙을 사람이나 공급업체에서 변경을 시켜주어야 한다. 즉, 동적이지 못하다는 이야기이다.

2. 침입방지시스템의 장점

침입차단시스템(방화벽)과 침입탐지시스템(IDS)에 이어 침입방지시스템(IPS:Intrusion Prevention System)이 제3세대 보안솔루션으로 주목을 받고 있다. IPS는 바이러스 웜이나 불법침입·분산서비스 거부공격(DDOS:Distributed Denial of Service) 등의 비정상적인 이상신호를 발견 즉시 인공지능적으로 스스로 적절한 조처를 취한다는 점에서 방화벽이나 IDS와 차별성을 갖는다. 즉 기존 IDS는 이미 알려져 있는 공격 시그니처를 감시하면서 수상한 네트워크 활동을 찾아내기 위한 목적으로 이상 네트워크 활동을 찾아냈을 경우 해당 운영 직원에게 경고 메시지를 보내고 침입의 진전상황을 기록하고 보고하는 것으로 끝나 문제를 즉각적으로 처리하지 못하는 데 반해 IPS는 침입경고 이전에 공격을 중단시키는데 초점이 맞춰져 있다. 특히 지난 코드레드 웜 피해 이후 IPS를 설치한 기업들이 피해를 전혀 입지 않은 것으로 알려지면서 더욱 각광을 받고 있다.[9]

공격에 대한 탐지만을 하는 침입탐지시스템의 한계성을 뛰어넘는 침입방지시스템은 공격 시그니처를 찾아내며, 서버에서 수상한 활동이 이뤄지는지를 감시한다. IPS는 서버가 비정상적인 행동을 실행하고자 하는 경우 자동으로 조치를 취함으로써 그것을 중단시킨다.

III. 침입방지시스템의 구현

침입방지시스템은 기존의 침입탐지시스템에 방화벽의 개념을 합쳤다는 개념보다는 좀 더 진보적인 것이다. 네트워크 상에서만 동작하는 네트워크 기반의 침입탐지시스템이나 방화벽, 그리고 호스트 기반에서 동작하는 호스트 기반의 침입탐지시스템이나 보안 운영체제(Secure OS) 들의 장점들을 모으고 또 다른 관점에서의 보안기능들을 합쳐놓은 것이라 할 수 있다.

1. 구현 시 고려해야 할 사항들

1) 호스트 기반의 방어

고속 네트워크, 스위칭, 그리고 단 대 단 암호화(end-to-end encryption)들과 같은 기술이 널리 이용됨에 따라 네트워크 단위의 보안에 대한 요구가 수시로 변화하고 있다. 무엇보다 확실하게 보안을 강화할 수 있는 곳은 실제 작업이 이루어지고 잠재적인 위험요소가 가장 큰 데스크탑이나 서버와 같은 호스트이다. 따라서 호스트 기반에서의 침입차단 기능을 강화해야 할 필요성이 있다.

2) 실시간 방지 결정

고도의 보안능력과 호스트의 보안정책을 우회할 수 있는 가능성을 줄이기 위해서는 응용프로그램은 반드시 정책기반의 확실한 탐지기능이 존재하는 커널레벨에서의 검사를 통과해야 한다. 효과적인 침입방지방법은 실시간으로 위반행위를 잡아야 하고 그러한 공격이 행해진 후에도 시스템에 공격의 효과가 생기지 않아야 한다.

3) 다양한 방법을 통한 공격방법에의 효과적인 방어

조직의 보안정책을 확실하게 반영하기 위해서는 침입방지시스템은 응용프로그램과 시스템간에 행하여지는 모든 중요한 통신개체들을 놓치지 않아야 한다. 네트워크 통제는 반드시 클라이언트/서버 통신에서의 포트간과 프로토콜 레벨까지 모두를 포함시켜야 하고 파일시스템 제어에서는 개인이나 그룹기반으로 쓰기와 읽기를 각각 허락하거나 거부할 수 있어야 한다. 레지스트리 제어에서는 중요한 레지스트리 정보에 대해서는 덮어쓰기나 변조가 허용되지 않아야 한다.

완벽한 침입방지 전략은 이처럼 다양한 방법에 대해 대비할 수 있어야 한다. 그래야 새로운 공격방법이 나타난다 할지라도 쉽게 대처할 수 있기 때문이다.[2]

4) 에이전트와 엔터프라이즈 레벨에서의 실시간 상관성 예측 (Correlation)

상관성 예측은 침입방지시스템의 생명이다. 에이전트에서 전개되는 상관성 예측은 방지결정의

수준을 높이는 데에 중요한 역할을 한다. 흩어져 있는 에이전트에서 모인 상관성 예측 정보는 종합적인 측면에서 다양한 자원들에 대한 보안정책을 쉽게 변경할 수 있도록 도와준다.[3]

5) 행동적 목표

침입방지의 목표는 보안정책이 침입이 시작된 뒤에 적용되는 것이 아니라 시작되기 전에 대책을 세워놓는 것에 있다. 침입 시그니처 값에 의한 방법은 항상 그 시그니처 값들의 갱신에 의존된다는 것이다.

6) 독특한 협동적 욕구를 충족시키는 융통성

모든 조합은 그 시스템과 관련 응용프로그램을 어떻게 구성을 하고 어떻게 관리하느냐에 따라서 상세한 것까지 같아야 한다. 고려되어야 하는 침입방지 방법은 독특한 적용과 도구들을 공급하는 새로운 정책을 만들고 그 정책의 실용화를 수용함으로써 이러한 특이성을 적용하기 위한 융통성이 있어야 한다. 이 해결법은 수동적으로 만들어진 정책의 운영적 모순들을 완화하기 위해 자동화된 정책 창출을 지지해야 한다.[3]

7) 전략 완화

침입방지 방법은 에이전트에서 이루어지는 방법과 관련된 개인적 경비를 최소화해야 한다. 고려되어야 하는 해결법은 이상적인 안전 정책의 빠른 전략을 예측하기 위해 추측기법을 제공해야 하고 다수에 의해 부가적인 방해 없이 요구되는 대로 발생하는 새롭고 소비적인 정책을 수용해야 한다.

8) 집중된 이벤트 관리방법

에이전트들에 의해 처리되는 모든 이벤트들은 경보와 기록이 저장되고 처리되는 집중된 저장소로 수집되어야 한다. 수집방법으로 고려되어지는 방법에는 SNMP, Paging, E-Mail 과 같은 일반적인 방법에 따르며 작동 시스템에 쉽게 적용할 수 있어야 한다.

9) 데스크탑과 서버들을 지원하는 플랫폼 지원방법

생각해야 할 해결책들은 반드시 조직이 방어를 원하는 운영체제를 지원해야 한다는 것이다. 님다(NIMDA)와 같은 여러 호스트를 동시에 목표로 하는 최근 공격들을 생각해 볼 때, 같은 관리방법과 강력한 패러다임이 한꺼번에 적용되어야 한다.

10) 관리

용이한 정책관리를 위해 정책들은 반드시 중앙집중식으로 결정되고 자동으로 모든 에이전트들에 적용되어야 한다. 정책들은 또한 보관되어질 수 있어야 한다.

한 명 이상의 관리자가 존재하는 조직에서는 그들의 환경에 적절할 수 있도록 어디에서든 관리를 할 수 있도록 지원하는 정책을 펴야 한다. 침입방지 방법은 관리용 프로그램을 관리자 컴퓨터에 깔게 되는 번거로움과 보안성의 이유로 보통 웹브라우저로도 간단하게 관리할 수 있도록 지원을 해야 한다.

수많은 에이전트를 보유하고 있는 조직에서는 한번에 수많은 에이전트를 관리할 수 있도록 지원하는 방법이 필요하다.[3]

IV. 결론

침입방지 시스템은 앞으로 침입탐지 시스템에 이어서 새롭게 등장한 정보보호 시스템 중에 하나이다. 이 논문에서는 침입방지 시스템을 구현하는 사람들이 참조해야 할 것들을 기술하고 있다.

침입방지시스템은 자원별 접근제어, 서비스네트워크 침입방지, 침입 경보, 침입 감사, 통합 관리, 로그 분석 등의 여러 가지 일들이 한꺼번에 처리되는 것인 만큼 다양한 보안기술을 가지고 있어야 한다.

현재 여러 회사에서 침입방지시스템을 개발하여 출시하고 있다. 하지만 아직 침입방지시스템의 표준화가 되어있지 않았다. 앞에서 제시한 참고사항들을 이용하면 보다 효율적이고 강력한 침입방지시스템이 완성되리라 생각된다.

참고문헌

[1] Jeff Schultise, Intrusion Prevention as Logical Evolution from Intrusion Detection, GSEC Assignment Version 1.2f, Dec 11, 2001.

[2] Xinyuan Wang, Douglas S.Reeves and S.Felix Wu, *Tracing Based Active Intrusion Response*

[3] Okena, *Technology Best Practices for Intrusion Prevention*, www.okena.com 2001

[4] Clarkin Michael, *Comparison of CyberwallPLUS Intrusion Prevention and Current IDS Technology, Network-1 Security Solutions*, Waltham, MA 2001

[5] Armored Networks Corporation White Paper *"Intrusion Prevention Evolution"*, 2001

[6] Andress and Mandy, *Intrusion Prevention: The Ultimate Security?*, 2001

[7] Firewall , http://www.terms.co.kr/firewall.htm

[8] http://www.ekardia.com/5_securitynews/press release.asp?tb=sn_press&GotoPage=3

[9] http://www.kisa.or.kr/K_trend/KisaNews/2001 12/infosec_trend_in.html